Smart Technologies Academic Press

Journal of Cyber Security and Risk Auditing

https://www.jcsra.thestap.com/

Robust Image Steganography against Differential Attacks Using GA-Optimized LSB Embedding

Dena Abu Laila[1*], Ziad E. Dawahdeh[2], Amer Alqutaesh[3*], Ghada Alradwan[3]

[1]*Faculty of Information Technology, Zarqa Technical Intermediate College, Zarqa University, Zarqa, Jordan.*

[2]*Computer Studies Department, Arab Open University, Amman, Jordan*

[3]*Deanship of Development and Quality Assurance, King Faisal University, 31982, Al-Ahsa, Saudi Arabia*

ARTICLE INFO

Article History

Received: 02-01-2026
Revised: 26-03-2026
Accepted: 01-04-2026

First Online

DOI:

***Corresponding author.**
Email:
dabulaila@ztic.edu.jo and aalqutish@kfu.edu.sa

Orcid:
https://orcid.org/0009-0000-7695-3930

This is an open access article under the CC BY 4.0 license (http://creativecommons.org/licenses/by/4.0/).

Published by STAP Publisher.

ABSTRACT

Recently, in the science of data hiding, most research papers propose several techniques to conceal data inside the images and ensure secure mediums such as text, images, audio, and videos with preserving its quality. Researchers have been interested in the last decade of these techniques in image steganography and cryptography, this research proposed a system that uses multiple layers of security in which steganography and cryptography are together to enhance security. This study aims to present a new efficient technique for hiding a gray image inside a blue layer of color image by combining the genetic algorithm (GA) with the Least Significant Bit (LSB) approach to optimal solution permutation for embedding pixel assortment of the image where data is to be concealed. This technique offers immovability differential attacks that are evaluated by several performance metrics. According to experimental findings, the stego and the cover image are visually indistinguishable. PSNR, MSE, and SSIM are used as measurement matrices. Our aim passed a successful test of robustness against experimental analysis.

Keywords: Image Steganography, Chaotic, Spatial Domain, Stego Image, Image Processing, Encryption, LSB, Genetic Algorithm.

How to cite the article

1. Introduction

Due to a rapid increase in cyber espionage via the internet, which led to a greater share of data being shared in digital form, data security has recently received more attention. Transferring this digital data through computer networks [1] isn't simple, usually without interruption or error. Concerns over the ability of data to be manipulated and attacked by third parties have grown as a result of the wide diffusion of data [2]. As a result, methods for preserving the security of secret communication are a crucial area of research, and related techniques grow in quantity and methodology every day.

The technologies adopted to protect confidential information from unauthorized access are encryption and steganography. They assist in ensuring data security. Cryptography is concerned with converting the content of the message to ciphertext to be unreadable to users, whereas Steganography is related to concealing communication by enclosing the messages behind a cover. However, encryption is not enough, and the visual transfer of confidential data between individuals can reveal the sender's and recipient's information to a potential attacker. In addition, the presence of encrypted data may tempt attackers to attack the secure transmission. The skill base on how to deal with these problems is steganography [28] [29].
Two layers of protection for confidential data are provided in our proposed model, which fully meets the requirements of an information security system, including confidentiality, integrity, authenticity, and non-repudiation by applying encryption and steganography to the image. This research aims to create a secure steganography technique that satisfies three requirements:
Robustness is an important element that could have a big impact on the steganography algorithm. This phrase refers to the message's ability to remain visible when a steganography image is vulnerable to a variety of planned or accidental attacks, like cropping, noise reduction, and compression. The technique is termed robust if the message survives attacks; otherwise, it is considered fragile.
Perceptibility is the most crucial aspect to consider when encoding a message in an image. This indicates that the viewer shouldn't be able to see the edits made to the host image after the embedded message. The confidentiality requirement of steganography will be violated if the modifications are observable to the naked eye.
Capacity: Increasing the number of hidden data points without sacrificing image quality is also crucial. To verify the quantitative measure, bits per pixel (bpp) and any performance metric, such as the PSNR or SSIM, may be employed to evaluate the caliber: high Robustness, non-perceptibility, and high capacity to introduce a new steganography method.

The main contribution of this work can be summarized as follows:

- The proposed method advances the field of methods for image steganography by offering a safe framework for the transfer of private data in a variety of applications.
- We proposed the genetic algorithm GA to find several solutions as a stego image. Which has numerous good or almost optimal solutions, and can display as many stego images as the user desires.
- Our method has a large embedding capacity and non-perceptibility compared with the author's literature.
- The recommended method selects the threshold for this criterion in a way that yields a set of acceptable embedding coefficients, the quantity of which may exceed the length of the data.

The remainder of the paper is organized as follows: Section 2 includes a literature review. Section 3 presents the proposed work and the testing and assessment mechanism in detail, with results and a discussion in Section 4. Section 5 concludes.

2. Literature review

There are several techniques to hide data, and they all use distinct strategies to successfully hide information. The following are some noteworthy methods for hiding data, some techniques in cryptography and steganography, and related works.

2.1 Types of Hidden Data

There are several ways to hide data, including watermarking, cryptography, and steganography, all of which are used in the science of data hiding. There is no clear difference between the science of cryptography and watermarks, Figure 1 below shows methods to hide data.

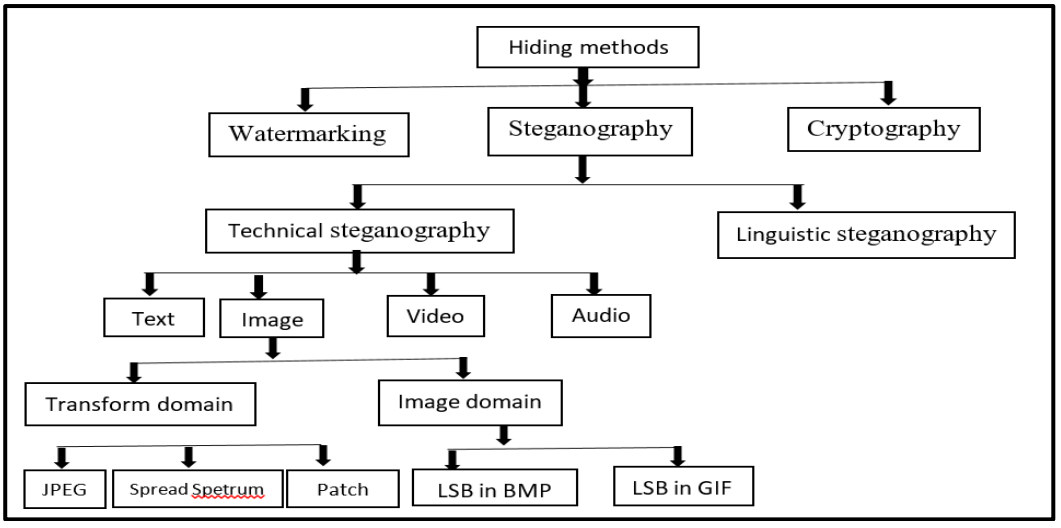


Figure 1. Ways to hide data.

Watermarking and Steganography are related technologies. Steganography during point-to-point communications (between sender and recipient), generally, one-to-many watermarking technology is used. Watermarking has been used on coins and stamps for many years to assist in spot counterfeiting. It is a translucent image that is printed on paper to ensure authenticity. The primary goals of digital watermarking are to guarantee digital media authentication and intellectual property rights [3]. Steganography, in its literal translation, "covered writing," is mainly used to hide information within any cover medium. Steganography deals with encryption in a way that accompanies both the process of encryption and decryption. But Steganography excels in encryption because it does not attract attention, while encryption is visible to the naked eye, regardless of whether it is broken. In countries and places where the use of cryptography for public purposes is restricted, steganography may be helpful for hidden communications.

2.2 Steganography

It is a procedure of concealing an image, sound, text, or video inside of another file, it is used to conceal transmission data. To shield the message from hackers' awareness. Every steganography system has two components: the message is initially concealed by the sender inside a cover object, and it is then decoded by the recipient. To create a stego-object that resembles the original cover object, after being converted to a binary message, the message is embedded into the host image or cover object. The binary message is extracted after the recipient transmits the stego-object across a public channel. Using a key at any point during the embedding process is not necessary. If the preferred method of steganography. Figures 2 and 3 below show the steganography system's extraction and embedding algorithms, respectively.

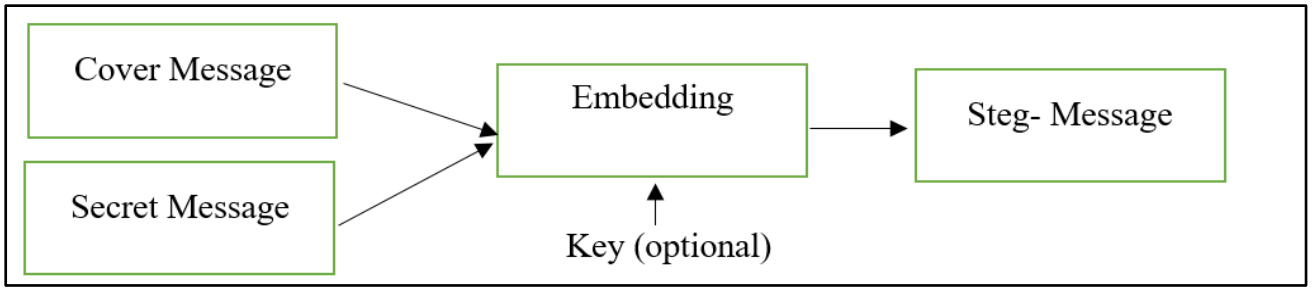


Figure 2. Embedding Algorithm

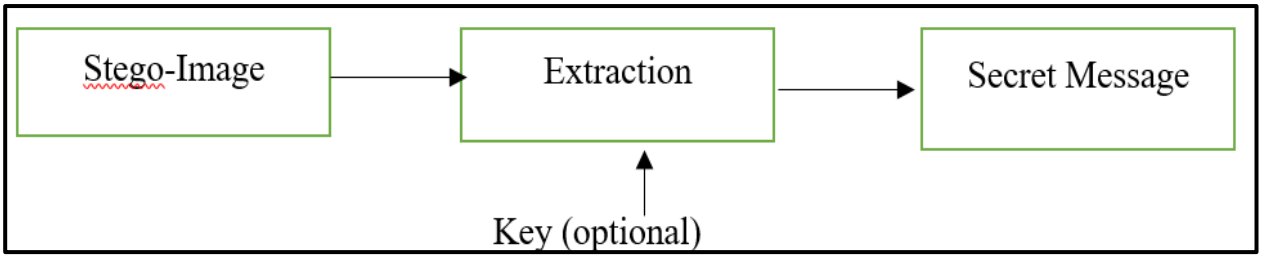
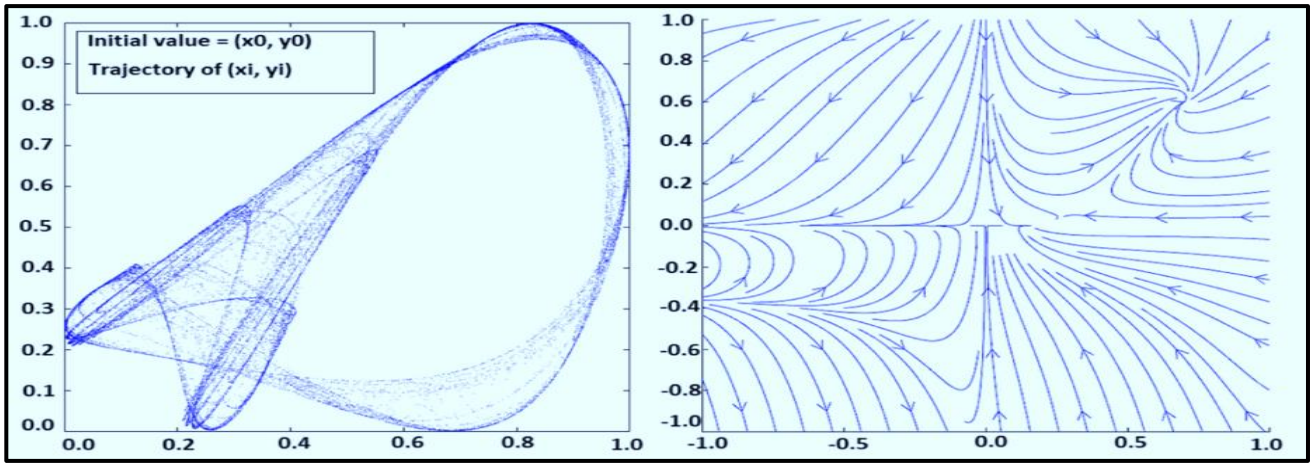


Figure 3. Extraction Algorithm

2.3 Cryptography

Encrypting the image data is necessary to ensure the transmission process's security. Due to the risk of transferring private information via a public [4]. Looking for one image encryption method, the practical approach is to handle the image in digital form as a binary stream, and then encrypt it using data encryption techniques [5]. And then a few binary files often represent the pixels of a digital image. Between adjacent pixels, there are high-frequency bits and linkages. As a result, image encryption may not be a good fit for conventional digital data encryption algorithms. Many image encryption techniques have been created, considering the attributes of the image [6]. The P-Fibonacci-based wave algorithm [7], the Transformation-based algorithm [8], the Chaos-based algorithm [9], and nearly are among the algorithms.

Numerous Image encryption techniques, including those based on quantum theory, DNA coding, and chaotic cryptography, have been presented by researchers as solutions to this issue [10]. Chaos cryptography is more suitable for cryptography with unique characteristics. It is a diverse field that incorporates the notion of chaos into cryptography [11]. Two types of chaotic maps exist: 1D chaotic maps and high-dimensional (HD) chaotic maps. The maps that are described as 1D chaotic in [12] are the Chebyshev, Sine, and Logistic maps. Among the shortcomings of 1D chaotic maps is that they have a simple architecture, few parameters, and limited information collection. Additionally, it is possible to forecast their chaotic orbits, parameters, and initial values. In this research, the 2D logistic chaotic map algorithm proposed has great results and is the most plays a vital role when compared to other Algorithms because it uses a plain image as the starting point before changing the order of the pixels. Image security is infused with discrete chaotic behavior and deterministic behavior. The most important and desired quality in image security is the ability to reverse chaos applied to image data. Figure 4 displays the phase portrait image of the 2D logistic map when r is adjusted to 1.19 th. The path composed of (x, y) has a completely random direction. It's also essential to know the numbers (x0, y0) and r [13].



(a)A two-dimensional logistic map trajectory (b) a 2D logistic map phase portrait

Figure 4. The 2D logistic map's behavior [14]

2.4 Genetic Algorithms (GA)

The Genetics algorithm is now widely used as an adaptable method that offers a randomized, parallel, and global search. It uses the principles of natural selection and genetics to base its search for an exact or nearly correct answer to a given optimization issue. GA is performed as a digital simulation, Where a population of abstract models for candidate solutions to an optimization problem. The first generation of evolution typically consists of a few genes chosen at random. All genes in a generation are considered a population. We refer to each individual in a population as a chromosome, also the fitness function is used to assess each chromosome's quality. As shown in Figure 5 There are four steps used to combine a new generation to choose the best result. The process is repeated until a predetermined condition is met. Once the fitness function and genetic representation have been established, the pseudocode algorithm of GA is illustrated, and the following steps.

Step1. [Initialization] Generate the initial population.
Step2. [Evaluation] Use the PSNR fitness function to evaluate each individual in the population.
Step3. [New Generation] Follow these instructions again until you get there.
Step 3.1 [Selection] Select the most qualified individual to reproduce.
Step 3.2 [Crossover] Choose two chromosomes at random to cross over, to avoid the offspring becoming an exact duplicate of the parents' two chromosomes.
Step 3.3 [Mutation] Using a mutation likelihood, the chromosome's location or chromosome's genes are chosen for a mutation.
Step 3.4 [Evaluation] Utilize the fitness function to assess each offspring.
Step 3.5 [Replacement] Replace the old population with the newly generated offspring.

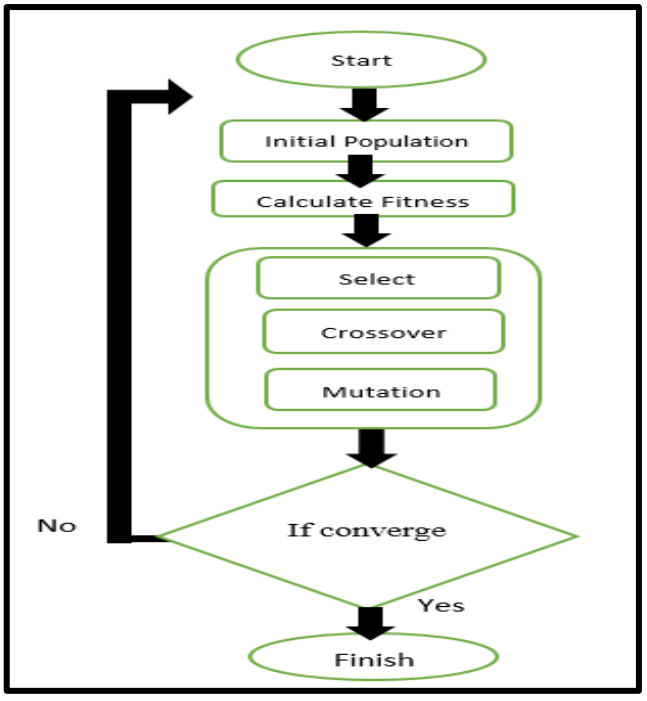


Figure 5. Basic Genetic Algorithm flowchart

2.5 Related Works

This section includes an analysis and discussion of several pertinent papers that have advanced the field of steganography techniques. [15] Presented two methods to convert every bit of the fifth-bit cover image into a hidden message for every pixel. The second technique identifies the optimal substitution matrix when incorporating confidential data by integrating the local pixel adjustment process (LPAP) with an evolutionary algorithm, thereby enhancing the quality of the stego-

image. By employing MSB to disguise the data rather than the optimal substitution algorithm and local pixel change, this method showed a sound substitution choice for storing and transferring important data. [16] They introduced an approach that chooses the cover image's LSB randomly. Pseudo-random encoding is used to embed secret data. The result demonstrates a maximum value of PSNR, imperceptibility, and robustness in terms of capacity when compared to the LSB technique. Furthermore, the PSNR of the suggested algorithm is greater than that of the LSB methods. [17] They improved the stego-image quality and the capacity to incorporate the crucial information from the secret message by implementing a data-hiding strategy that leveraged fundamental LSB. The secret message is implanted when the message from the secret bits instantly changes the rightmost k LSBs of the pixels in the host image. The host image is divided in half: the first half identifies the changes made to each pixel that already exists, while the second half embeds the secret information of the message and modifies the bit values using an LSB replacement to extract the secret bits. [18] Proposed employing the idea of a non-linear dynamic system to encrypt the message's secret bits (chaotic). To improve protection against attacks, every component of the secret image is encrypted using a unique chaotic sequence before being incorporated into the cover image. A method known as 3-3-2 LSB embedding has been used for image steganography. Finally, a very optimistic performance analysis is found for the proposed technique. Use the recommended procedure with JPEG files. [19] Suggested to use of an AES to encrypt the secret data and to present a novel algorithm for word and image embedding into videos. This algorithm would select the best video tags to conceal text and the best frames and pixels to place photos. Consequently, the video's size and visual quality remain unchanged even after adding hidden content. [20] Employed a genetic algorithm to embed 3 bits of each byte by 3x3 masks generated from the source color image utilizing the spatial domain technique. This improved PSNR over the previous method. [21] Proposed Pixel Value Differencing (PVD) Steganography in Grayscale. In this strategy, they are using non-overlapping 1 x 2 pixel blocks. The pixel difference of the block is measured and replaced with a new value corresponding to secret data. Another method makes use of PVD with modulus function (PVDMF). [22] The introduction of the innovative technique in LSB steganography optimization, which complements logistic chaotic maps with genetic algorithms, was promising. Their approach showed to deliver a noticeable improvement to imperceptibility and security over conventional LSB approaches. Nevertheless, their strategy was dedicated mainly to the grayscale images embedding, leaving out the domain of incorporation in color images and channel-wise approaches. Moreover, they used a genetic algorithm version, which was single-objective, conserving the possibility of multiple performances. Based on these premises, we present in this paper an upgrade of the chaos-GA combination by involving both multi-objective optimization and blue-channel exploitation, and the evaluation of the security of the proposed tool against sophisticated steganalysis methods.

3. Research Methodology

The proposed research involves hiding a secret grayscale image inside a color image using the principle of least significant bits (LSB). However, with the release of algorithm details, an attacker could determine the number of LSBs used, potentially leading to the discovery of secret information. To counter this, a logistic map is employed to generate a pseudorandom pattern of numbers, which is then used to encrypt the secret image. Additionally, to reduce image distortion, the steganography embedding method is optimized using a genetic algorithm. The MATLAB R2021a environment was used to accomplish the suggested method. We utilized a Dell Core i7 Intel CPU, 16 GB of RAM, Windows 11, and a 64-bit operating system.

3.1 Encryption Method

The steps that follow outline the processes of the encryption algorithm in Algorithm1.

Algorithm 1. Encryption Algorithm

1. Generate a random encryption key to regulate the pseudo-random sequence obtained from the 2D logistic map.
2. Use a 2D Logistic Permutation Algorithm to rearrange the Xseq and Yseq components.
3. Utilize the finite field logistic diffusion.
4. Use the logistic transposition in 2D.

Figure 6 shows the flowchart for the suggested image encryption approach, which uses a 2D logistic map. Two-dimensional logistic diffusion, two-dimensional logistic transposition, and 2D logistic permutation constitute the internal loop. Because they build a network of substitutions and permutations, each of these functions acts as a standalone picture cipher. The decryption just reverses the processing sequence while using the decryption key, as Figure 7 illustrates.

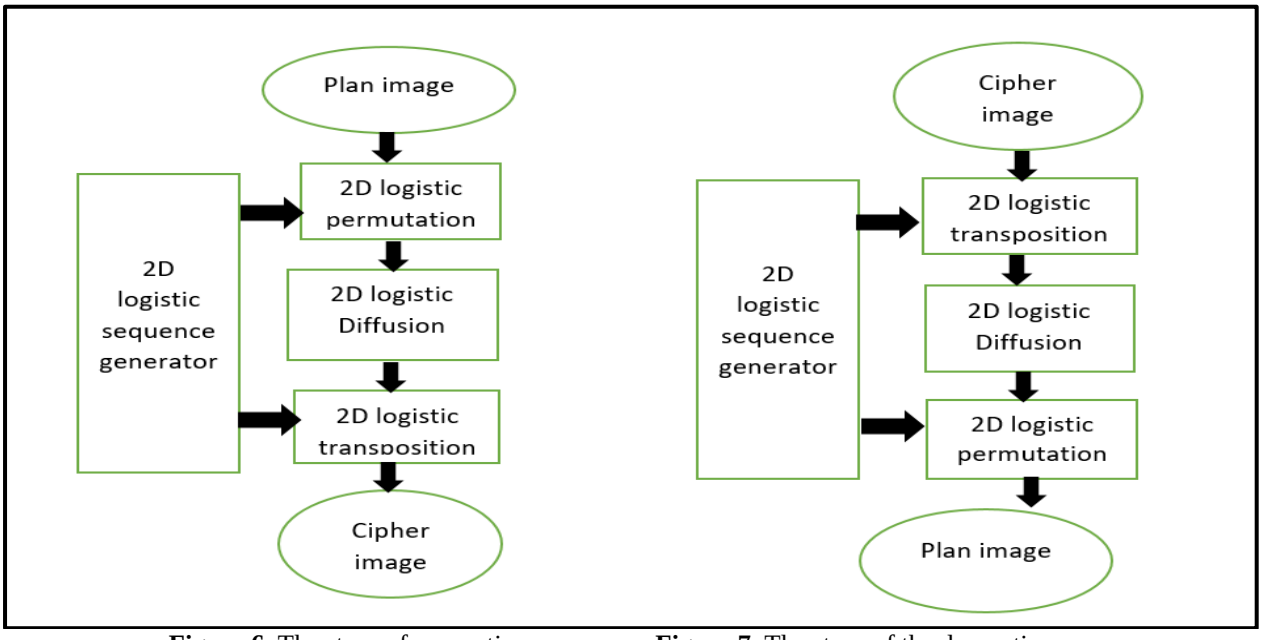


Figure 6. The steps of encryption by the 2D logistic map

Figure 7. The steps of the decryption by the 2D logistic map.

3.2 Embedding Algorithm

The specifics of the embedding procedure are explained in this part. In this research, LSB and GA are both provided as methods for concealing images. To convey all of the secret data, a novel steganography technology is used. The suggested method is a cutting-edge, dependable way to assign secret data to the blue channel of a color image, as shown in Figure 8. The suggested approach utilizes the complex behaviors that arise from basin and attraction evolution using a GA to select the best locations to embed the secret bit.

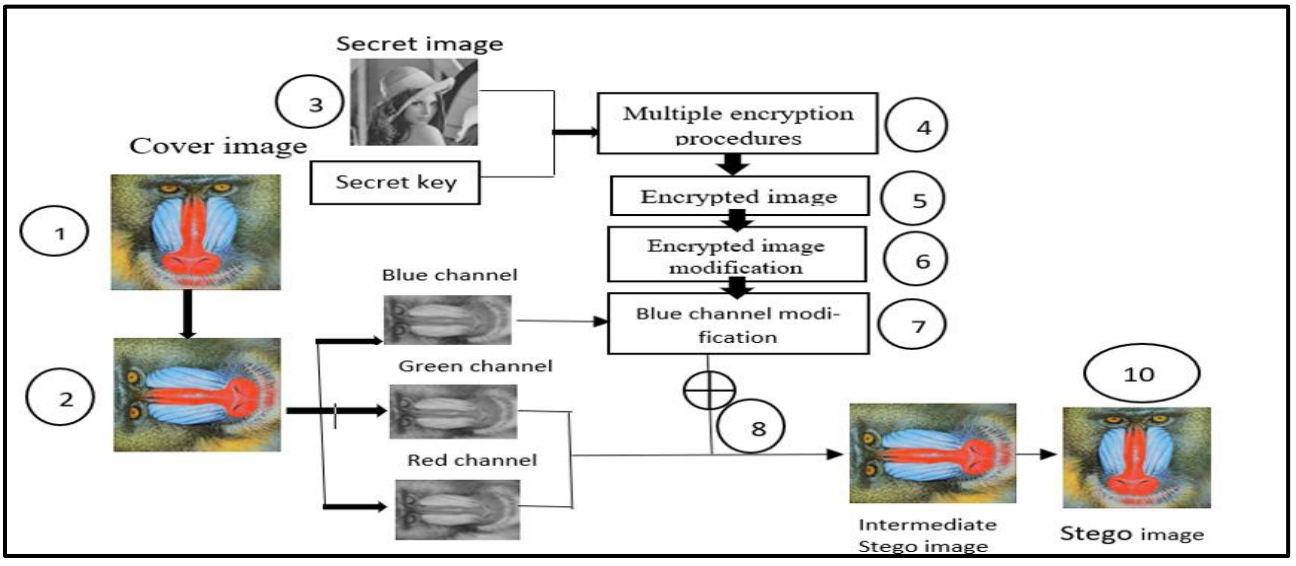


Figure 8. Overall representation of the proposed framework

The proposed technique needs a color cover and a gray secret image to give a stego-image that is sent to the receiver. Algorithm 2 explains the steps explain the embedding algorithm.

Algorithm 2. embedding algorithm

1. Read the host images then apply image rotation (270^0).
2. Divided the image into 3 matrices R, G, and B.
3. Convert the secret encrypted image to (M ×N× 8) row vector.
4. Split each pixel of the secret image into 2- blocks.
5. Apply genetic algorithm.
6. Replace the 4-LSBs in the cover image with secret pixels.
7. Bring the three layers together
8. Apply reverse image rotation (270o) for the host image.
9. Get a stego-image.

When we get the encrypted image, each pixel consists of 8 bits, and each pixel block must first be divided into two parts to be included in the cover image. Before the embedding process is done, the optimal permutation is obtained from the genetic algorithm (GA) for the secret message derived from the global best chromosome that can obtain the best PSNR. The next step, replacing the secret encrypted bits with bits of the host image. If we have 4 bits then we have 2^4 =16 possible values to replace which values (0-15). Assume we want to embed (0111) and (0001) as shown in Fig 9, to pixel's value 200 (in decimal 11001000), and 13 (0000**1101**) then should swap out the hidden image's 4-bit blocks with the cover image's 4-LSBs. but before it, the genetic algorithm will choose the best value to replace the secret bit with its. Figure 9 explains it.

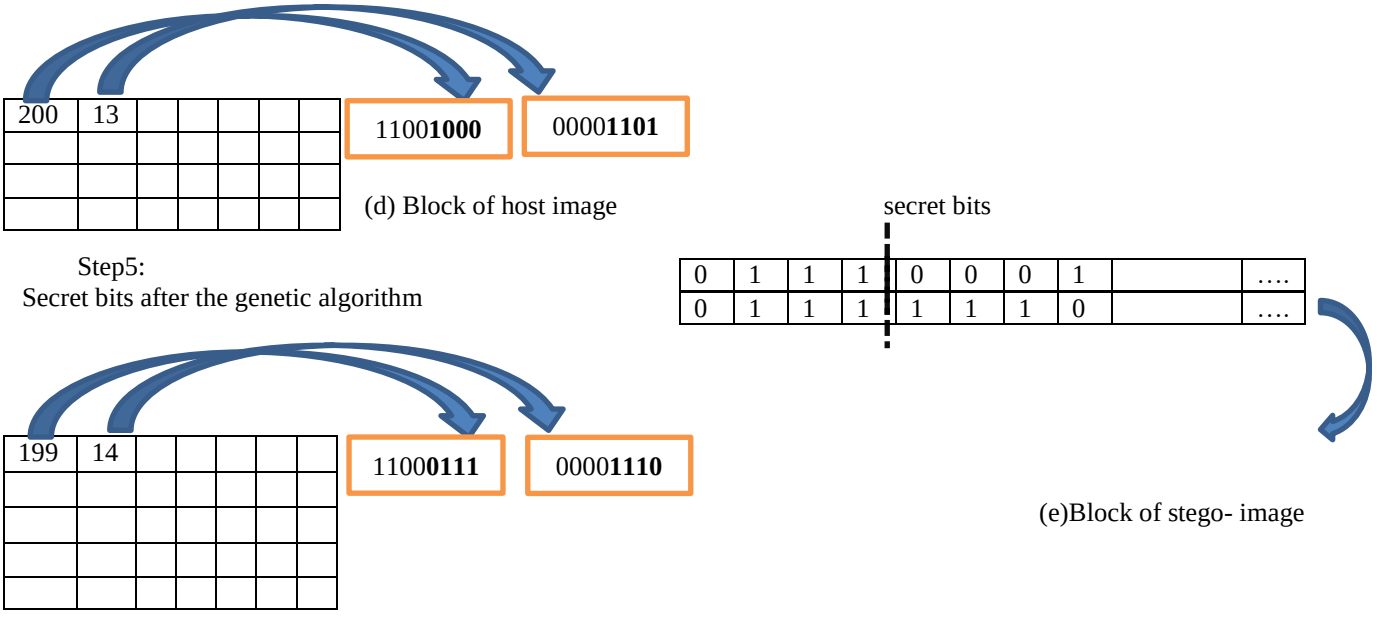


Figure 9. The encoding process of the proposed encoding Secret Image with a Cover Image.

3.2.1 Scanning order in the host image

Algorithm 3. for scanning order

1. Determine the population and iteration size.
2. Start scanning from any position.
3. Calculate the fitness function for each round.
4. Repeat the scan depending on the number iteration.
5. Select the best location to start from.

The place where information can be withheld with the least chance of it being distorted is referred to as the ideal spot. To hide the message bits, this approach defines the initial pixels, the amount of LSB used within a single pixel, and the order in which the image pixels are scanned. The pixel order of the host image is used as Pixel raster order in the LSB substitution technique. There may be a better order among the ones displayed in Figures 10 and 11, with Figure 10's order outperforming the raster order. Consequently, every time a randomly chosen place is chosen, the capacity is checked. There are multiple initial hiding spots for the hidden image in the host picture. The number of pixels in the.

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25

Figure 10. Raster order.

20	21	22	23	24
25	1	2	3	4
5	6	7	8	9
10	11	12	13	14
15	16	17	18	19

Figure 11. Raster order.

3.2.2 Genetic algorithm

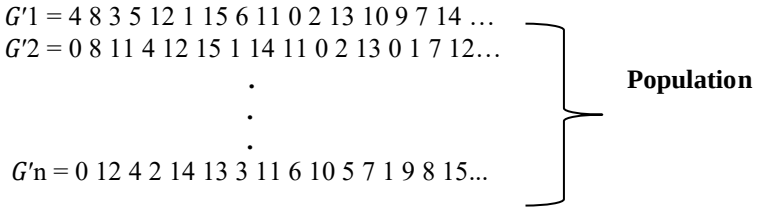
This technique is more effective when the value of k > 3 because it will contain enough numbers to choose alternatives to another k_bit. For example, in the proposed method when k = 4 there is a probability of 2^4 to transpose the last 4 bits (0-15) in each pixel, which is called genetic, and many numbers of random chromosomes. For example, in the gray secret image of size 128 * 128, when converted to a vector, the block size will be 32768 individuals of a population, and values of individuals range from 0 to 15, which leads to a high probability of bit flipping. The next section explains it.

3.2.2.1 Create and select the initial population

Algorithm 4. Create an initial population

1. Select the number of the population.
2. Create random genes of size (M×N×2) for each chromosome.
3. Evaluate cost by calculating PSNR for each chromosome.
4. Sorting the chromosomes by a cost function
5. Select the best chromosome wish has a high value.

Creating the initial population is the first step in the GA process. To create offspring for succeeding generations, this population has been chosen in the next step to go through the processes of crossover and mutation. The fitness function is then used to assess each offspring's quality, and the offspring with the best quality is permitted to survive and influence the following generation. All that is done again until a predetermined threshold is achieved, or a predetermined condition is satisfied. If we select a random chromosome, we can create a sample population as



Competition selection is the process used to choose a person from the population. There are numerous individuals (chromosomes) in this place, and after choosing the winners of each competition, mutation and cross-over are used to identify the best member worldwide [30-33]. The PSNR of each substitution is calculated by this algorithm, which then chooses the one with the highest PSNR value. It is common practice to employ the genetic algorithm, which randomizes the search process [34-40]. As you compare the host image and the stego image, find the PSNR value of each pixel. Table 1 displays the Pixels of the original image, as demonstrated in Table 2 the Pixels of the secret image. One pixel of the host image contains every four bits of the secret image. The secret image's pixels must first be split into two halves. Then, each component switches to a new value base and selects the optimal chromosome using a genetic process.

3.2.2.2 Cross-over

Then make crossover and mutation to create new offspring. The first step randomly get chromosome (parent 1) and Obtain another chromosome based on chaos theory (parent 2) then make a crossover between them of the range 0.5 and change the position I and j for each other to calculate the value of fitness for each offspring if the fitness function (PSNR) is the best value chose this offspring and repeat it to another one depends on number iterations to make crossover and mutation.

Algorithm 5. Crossover algorithm

1. Select chromosome (parent 1) randomly.
2. Obtaining another chromosome based on chaos theory (parent 2)
   - Replace the parent 1 to parent 2 segment between the cut spot (of rate 0.5).
   - Get the position of each chromosome.
   - Replace the i value of parent 1 with the j value of parent 2 and the j value of parent 1 with the i value of parent 2.
3. Get offspring1 and offspring2.

3.2.2.3 Mutation

Algorithm 6. Mutation

1. Obtaining one chromosome based on chaos theory.
2. Change each value of each gene randomly.
3. Check the PSNR value, if it gets a larger value, it will be selected.
4. Choose two locations (value for pixels) based on logistic chaos.
5. Repeat the same process many times.

3.3 Extracting Algorithm

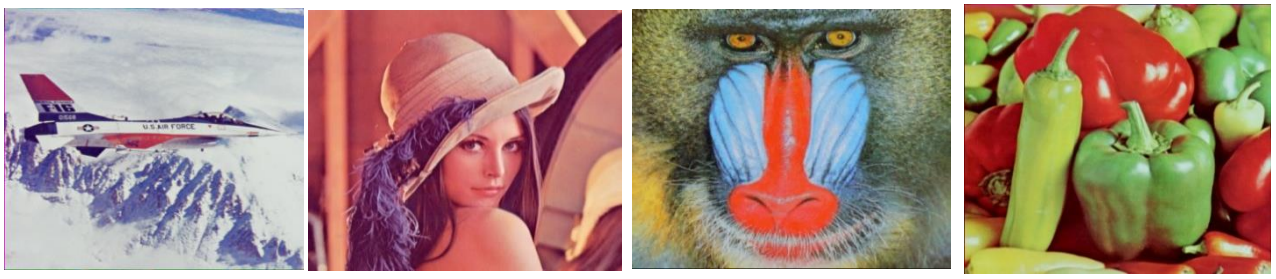
The method of extraction is the reverse of embedding. To extract the hidden secret image, the actions that follow are taken by the message receiver.

Algorithm 7. Extracting Algorithm

1. Read the stego image then apply image rotation (270^0)
2. Split the image into 3 matrices for each R, G, and B matrix.
3. The blue matrices stego image layer's pixel value should be changed to binary.
4. Extract the four bits from the pixel blue layer of the stego image.
5. Apply reverse genetic algorithm.
6. Store secret bits in an array.
7. Reshape the row vector to 8-bit.
8. Bring the three layers together.
9. Apply image rotation (270^o) for each R, G, and B matrix.
10. Decrypt the secret image.
11. Obtain the secret image.

4. Result & Discussions

The experimental findings based on multiple image quality assessment metrics are presented for performance assessment. The cover images for this experiment are "Baboon, Lena, pepper, and airplane" as indicated in Figures 12, the hidden images are "Lena," "mandrill," "jetplane,"," and "cameraman," as indicated in Figures 13, and the size of the images is 512 x 512.



Figures 12. Cover Image

Figures 13. Secret Images

4.1 Security Analysis of Cryptography

In this research, the PSNR, MSE, and SSIM were utilized to evaluate the stego image quality. Additionally, as demonstrated in the next sections a measure of capacity is how many secret bits are contained in the cover image.

4.1.1 Payload capacity and imperceptibility evaluation

Table 1 presents results that demonstrate that the suggested approach generates stego-images that retain high embedding rates and a high standard of quality to assess the efficacy of this approach where the 4-LSB value and baboon host image of size 512*512 with a maximum capacity up to 65k. The population size and iteration values for the genetic parameters in the proposed method are 50 and 50, respectively. Three instruments-PSNR, MSE, and SSIM-have been employed to measure image quality, and the results are displayed below. Table 1 shows the PSNR, MSE, and SSIM values for different secret image sizes.

Table 1. PSNR, MSE, and SSIM values for different secret image sizes.

Capacity (bytes)	Proposed Method			
	Image	**PSNR**	**MSE**	**SSIM**
4096 (4k)	Lena	71.2193	0.0051	0.99999701
	jet	71.1968	0.00493	0.99999692
	mandrill	71.2114	0.0049	0.99999693
16384 (16k)	Lena	64.4004	0.0236	0.99999031
	jet	64.9885	0.0236	0.99999025
	mandrill	64.9936	0.0205	0.99999024
65536(65k)	Lena	58.6239	0.0892	0.99995022
	jet	58.6061	0.0896	0.99995040
	mandrill	58.556	0. 0906	0. 99995057

As shown in Table 2, in the cover image "Baboon and Lena ", the experiment contrasts the embedding results from the techniques used by [23], where the PSNR Value is identical as 45.9625 to 49.21157dB, [27], for which the PSNR value was 40.0288 to 40.27397 dB [25], for which the PSNR value was 49.1581 to 45.62057 dB, [26], for which the PSNR value was 49.1557 to 45.61867 dB, [27], for which the PSNR value was 52.63973 to 52.6469 dB, and the suggested approach, which has a high PSNR value 63.3245 to 64.0044 dB when the number of embedding bits is (4,6 and 8k). The evaluation of the suggested plan with the other six SSIM-based methods in Table 3.

Table 2. Demonstrates the outcome of embedding the secret images

Image Name	**Secret data (KBs)**	**Cipher size in bytes**	**Classic LSB Method**	**[23]**	**[27]**	**[25]**	**[26]**	**[27]**	**Proposed Method**
Baboon image with dimension 256×256	4	4177	51.9039	46.5301	40.0609	49.3853	49.3783	54.1715	64.9358
	6	6499	51.4696	46.0068	40.0258	49.1359	49.1352	52.3963	63.0493
	8	8192	51.1648	45.3508	39.9997	48.9531	48.9536	51.3729	61.9884
	Average		**51.5127**	**45.9625**	**40.0288**	**49.1581**	**49.1557**	**52.6469**	**63.3245**
Lena with a resolution of 256×256	4	4177	45.7183	49.2242	40.3033	45.7193	45.7193	54.147	65.0213
	6	6499	45.6108	49.2061	40.2696	45.6128	45.61	52.3881	65.0213
	8	8192	45.53	49.2044	40.249	45.5296	45.5267	51.3841	61.9707
	Average		**45.6197**	**49.2115**	**40.27397**	**45.6205**	**45.6186**	**52.6397**	**64.0044**

Table 3. Evaluation of the suggested plan with the other six SSIM-based methods

Image Name	Secret bits (KBs)	size in bytes	Classic LSB Method	(Gutub, (2010))	[24]	[25]	[26]	[27]	Proposed Method
Baboon image with dimension 256×256	4	4177	0.9993	0.9984	0.9925	0.9994	0.9994	0.9999	0.99999
	6	6499	0.9991	0.998	0.9925	0.9993	0.9993	0.9998	0.999979
	8	8192	0.9989	0.9975	0.9925	0.9993	0.9992	0.9997	0.999955
	Average		**0.9991**	**0.9979**	**0.9925**	**0.99933**	**0.9993**	**0.9998**	**0.999967**
Lena with a resolution of 256×256	4	4177	0.9987	0.997	0.9818	0.9991	0.9991	0.9996	0.9999925
	6	6499	0.9981	0.9968	0.9818	0.9988	0.9987	0.9995	0.9999856
	8	8192	0.9977	0.9983	0.9818	0.9985	0.9984	0.9994	0.9999670
	Average		**0.998167**	**0.9973**	**0.9818**	**0.9988**	**0.9987**	**0.9995**	**0.999982**

4.1.2 Histogram analysis

The original and stego images differ in ways that are difficult to distinguish with the human eye. The RGB histogram (the pixel intensities' dispersion) for cover images and stego images was used to improve the comparability and assess the visual attacks. This is shown in Figure 14. It is evident from the original and stego image histograms that the RGB histograms of the two images appear to be similar.

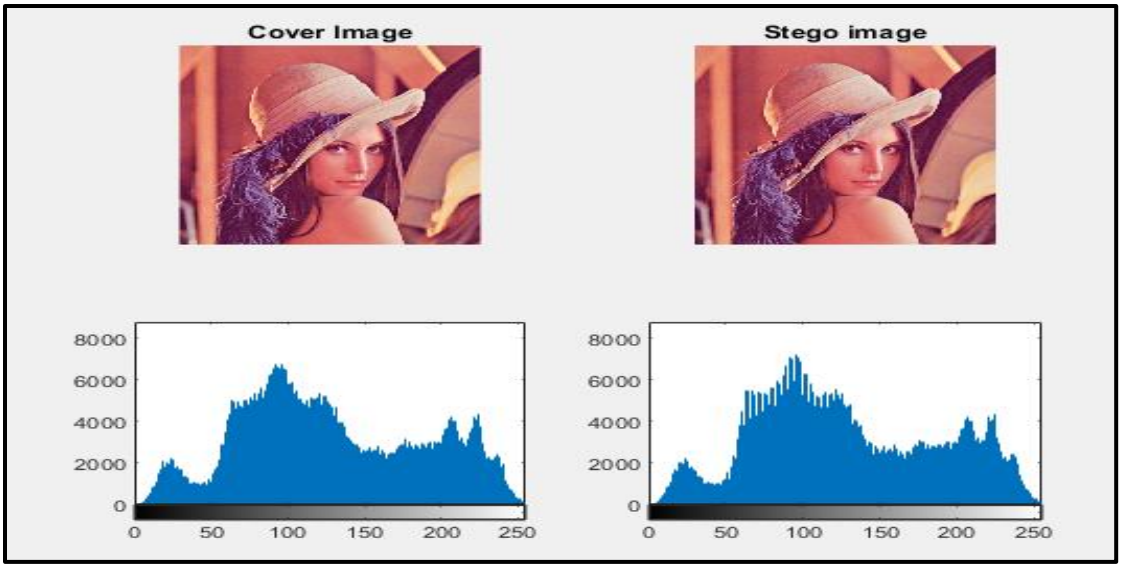


Figure 14. Lena inputs and outputs images with their histograms

5. Conclusion

This paper hides a secret gray image inside the color image using a steganography technique based on LSB and genetic algorithms. The proposed algorithm gave good results because it used many levels of the genetic algorithm. Using a genetic algorithm is far from the traditional method. The algorithm used an optimization process on many levels, trying to find the best objective function. According to experimental findings using test images from the USC-SIPI image database the stego-

image and the cover image are visually indistinguishable. The Visual quality of the image is measured by PSNR, MSE, and SSIM. The proposed method passed a successful test of robustness against experimental analysis. Additionally, when compared to the previous research, the comparative results of the suggested algorithm are quite encouraging. And we reached better results than previous studies in terms of capacity, incomprehensibility, strength, and increased metric values.

Corresponding author

Dena Abu Laila
dabulaila@ztic.edu.jo

Acknowledgements
This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Grant No. KFU261655).

Funding
This work was funded by King Faisal University.

Contributions
All authors contributed to the development and completion of the entire manuscript.

Ethics declarations
This article does not contain any studies with human participants or animals performed by any of the authors.

Consent for publication
Not applicable.

Competing interests
All authors declare no competing interests

References

[1] Laila, D. A., Al-Na'amneh, Q., Aljaidi, M., Nasayreh, A. N., Gharaibeh, H., Al Mamlook, R., & Alshammari, M. (2024). Simulation of Routing Protocols for Jamming Attacks in Mobile Ad-Hoc Network. In Risk Assessment and Countermeasures for Cybersecurity (pp. 235-252). IGI Global.
[2] Dhawan, S., & Gupta, R. (2021). Analysis of various data security techniques of steganography: A survey. Information Security Journal: A Global Perspective, 30(2), 63-87.
[3] Zhou, Y., Bao, L., & Chen, C. P. (2014). A new 1D chaotic system for image encryption. Signal processing, 97, 172-182. (Zhou, (2014))
[4] Khalaf, Y., Aljaidi, M., Laila, D. A., Alsarhan, A., Alkhawaldeh, A. K., Alsuwaylimi, A. A., & Kharabsheh, M. (2024). An Effective Encryption Algorithm Based on RSA and DES.
[5] Allasasmh, O., Laila, D. A., Aljaidi, M., Alsarhan, A., & Samara, G. (2024, December). Integrated Approaches to Steganography: Embedding Static Information Across Audio, Visual, and Textual Formats. In 2024 International Jordanian Cybersecurity Conference (IJCC) (pp. 33-39). IEEE.
[6] Almaiah, M. A., Maleh, Y., & Alkhassawneh, A. (Eds.). (2024). Risk assessment and countermeasures for cybersecurity. IGI Global.
[7]Panetta, K., Agaian, S., & Chen, C. P. (2012). Image encryption using P-Fibonacci transform and decomposition. Optics Communications, 285(5), 594-608.
[8] Liao, X., Lai, S., & Zhou, Q. (2010). A novel image encryption algorithm based on self-adaptive wave transmission. Signal processing, 90(9), 2714-2722.
[9] Enayatifar, R., Abdullah, A. H., & Isnin, I. F. (2014). Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence. Optics and Lasers in Engineering, 56, 83-93.
[10] Hua, Z., Zhou, B., & Zhou, Y. (2018). Sine chaotification model for enhancing chaos and its hardware implementation. IEEE Transactions on Industrial Electronics, 66(2), 1273-1284.
[11] Kanan, H. R., & Nazeri, B. (2014). A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm. Expert systems with applications, 41(14), 6123-6130.
[12] Jain, A., & Rajpal, N. (2016). A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps. Multimedia Tools and Applications, 75, 5455-5472.
[13] Dena Abu Laila, Qais Al-Na'amneh, Mohammad Aljaidi, Ahmad Nawaf Nasayreh et al. "chapter 10 Enhancing 2D Logistic Chaotic Map for Gray Image Encryption", IGI Global, 2024 [14] Iqbal, N., Hussain, I., Khan, M. A., Abbas, S., & Yousaf, S. (2023). An efficient image cipher based on the 1D scrambled image and 2D logistic chaotic map. Multimedia Tools and Applications, 1-29.

[15] V, G., G, I. A review on image steganographic techniques based on optimization algorithms for secret communication. Multimed Tools Appl (2023). https://doi.org/10.1007/s11042-023-15568-7.
[16] Hegde, R., & Jagadeesha, S. (2015). Design and Implementation of Image Steganography by using LSB Replacement Algorithm and Pseudo Random Encoding Technique. International Journal on Recent and Innovation Trends in Computing and Communication, 3(7), 4415-4420.
[17] Mohamed, M. H., & Mohamed, L. M. (2016). High capacity image steganography technique based on LSB substitution method. Applied Mathematics & Information Sciences, 10(1), 259.
[18] Bandyopadhyay, D., Dasgupta, K., Mandal, J. K., & Dutta, P. (2014). A novel secure image steganography method based on chaos theory in spatial domain. International Journal of Security, Privacy and Trust Management (IJSPTM), 3(1), 11-22.
[19] Selim, N. M., Guirguis, S. K., & Hassan, Y. F. (2022). Video steganography for image and text using deep genetic algorithm and LSB. International Journal of Network Security, 24(1), 140-146.
[20] Mandal, J. K., & Khamrui, A. (2014). A genetic-algorithm-based steganography on colour images (GASCI). International Journal of Signal and Imaging Systems Engineering, 7(1), 59-63.
[21] Ramakrishna, H. & Jagadeesha, S. (2015). Design and Implementation of Image Steganography by using LSB Replacement Algorithm and Pseudo Random Encoding Technique. IJRIT in Computing and Communication, Vol. 3 Issue 7, pp. 4415-4420.
[22] Laila, D. A., Aljaidi, M., Almaiah, M. A., AlBourini, M., Al-Na'amneh, Q., Samara, G., ... & Momani, K. (2025). A Novel Scheme to Optimize LSB Steganography Based on a Logistic Chaotic Map and Genetic Algorithm. Iraqi Journal for Computer Science and Mathematics, 6(2), 24.
[23] Gutub, A. A. A. (2010). Pixel indicator technique for RGB image steganography. Journal of emerging technologies in web intelligence, 2(1), 56-64.
[24] Jassim, F. A. (2013). A novel steganography algorithm for hiding text in image using five modulus method. arXiv preprint arXiv:1307.0642.
[25] Bailey, K., & Curran, K. (2006). An evaluation of image based steganography methods. Multimedia Tools and Applications, 30, 55-88.
[26] Karim, S. M., Rahman, M. S., & Hossain, M. I. (2011, December). A new approach for LSB based image steganography using secret key. In 14th international conference on computer and information technology (ICCIT 2011) (pp. 286-291). IEEE.
[27] Muhammad, K., Ahmad, J., Farman, H., Jan, Z., Sajjad, M., & Baik, S. W. (2015). A secure method for color image steganography using gray-level modification and multi-level encryption. KSII Transactions on Internet and Information Systems (TIIS), 9(5), 1938-1962.
[28] Al-Shareeda, M. A., Ali, A. M., Hammoud, M. A., Kazem, Z. H. M., & Hussein, M. A. (2025). Secure IoT-based real-time water level monitoring system using ESP32 for critical infrastructure. J. Cyber Secur. Risk Audit, 2, 43-52.
[29] Alotaibi, E., Sulaiman, R. B., & Almaiah, M. (2025). Assessment of cybersecurity threats and defense mechanisms in wireless sensor networks. J. Cyber Secur. Risk Audit, 2025(1), 47-59.
[30] Ali, A. (2024). Adaptive and context-aware authentication framework using edge AI and blockchain in future vehicular networks. STAP Journal of Security Risk Management, 2024(1), 45–56. https://doi.org/10.63180/jsrm.thestap.2024.1.3
[31] Chandak, A., & Chandak, P. (2026). Blockchain technology in health care: An extensive scoping review of the existing applications, challenges, and future directions. International Journal of Cybersecurity Engineering and Innovation, 2026(1).
[32] Addula, S. R., Norozpour, S., & Amin, M. (2025). Risk assessment for identifying threats, vulnerabilities and countermeasures in cloud computing. Jordanian Journal of Informatics and Computing, 2025(1), 38–48. https://doi.org/10.63180/jjic.thestap.2025.1.5
[33] Abu Laila, D. (2025). Responsive machine learning framework and lightweight utensil of prevention of evasion attacks in the IoT-based IDS. STAP Journal of Security Risk Management, 2025(1), 59–70. https://doi.org/10.63180/jsrm.thestap.2025.1.3
[34] Ibrahim, A., Kadhim, A. F., Hamzah, A. E., & Al-Shareeda, M. A. (2026). A secure and scalable IoT home automation architecture with web and biometric control. International Journal of Cybersecurity Engineering and Innovation, 2026(1).
[35] Alshinwan, M., Memon, A. G., Ghanem, M. C., & Almaayah, M. (2025). Unsupervised text feature selection approach based on improved Prairie dog algorithm for the text clustering. Jordanian Journal of Informatics and Computing, 2025(1), 27–36. https://doi.org/10.63180/jjic.thestap.2025.1.4
[36] Abu Laila, D., Aljawarneh, M., Al-Na'amneh, Q., & Bin Sulaiman, R. (2025). Optimizing intrusion detection systems through benchmarking of ensemble classifiers on diverse network attacks. STAP Journal of Security Risk Management, 2025(1), 71–84. https://doi.org/10.63180/jsrm.thestap.2025.1.4
[37] Alsahaim, S., Almaiah, M. A., & Sulaiman, R. B. (2023). Security threats in mobile phones: Challenges, countermeasures, and the importance of user awareness. International Journal of Cybersecurity Engineering and Innovation, 2023(1).
[38] Kareem, K. A., & Al-Shareeda, M. A. (2026). A low-complexity Li-Fi communication framework for short-range text transmission. Jordanian Journal of Informatics and Computing, 2026(1), 15–24. https://doi.org/10.63180/jjic.thestap.2026.1.2
[39] Alrajeh, M., Almaiah, M., & Mamodiya, U. (2026). Cyber risk analysis and security practices in industrial manufacturing: Empirical evidence and literature insights. International Journal of Cybersecurity Engineering and Innovation, 2026(1).
[40] Al-Na'amneh, Q., Aljawarneh, M., Alhazaimeh, A. S., Hazaymih, R., & Shah, S. M. (2025). Securing trust: Rule-based defense against on/off and collusion attacks in cloud environments. STAP Journal of Security Risk Management, 2025(1), 85–114. https://doi.org/10.63180/jsrm.thestap.2025.1.5